

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-247111

(P2002-247111A)

(43)公開日 平成14年8月30日 (2002.8.30)

(51)Int.Cl.	識別記号	F I	特許庁 (参考)
H 0 4 L 12/66		H 0 4 L 12/66	B 5 B 0 8 5
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 A 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 D 5 K 0 3 0

審査請求 未請求 請求項の数16 O L (全 9 頁)

(21)出願番号 特願2001-43512(P2001-43512)

(22)出願日 平成13年2月20日 (2001.2.20)

(71)出願人 595161887

エム・シー・エムジャパン株式会社
東京都世田谷区三軒茶屋2-11-22 サン
タワーズセンタービル

(72)発明者 奥藤 亨

東京都世田谷区三軒茶屋2丁目11番22号
サンタワーズセンタービル エム・シー・
エムジャパン株式会社内

(74)代理人 100109014

弁理士 伊藤 充

Fターム(参考) 5B085 A401 A602 A604

5J104 A407 K401 M402 P407

5K030 G415 H408 B01 H103 H006

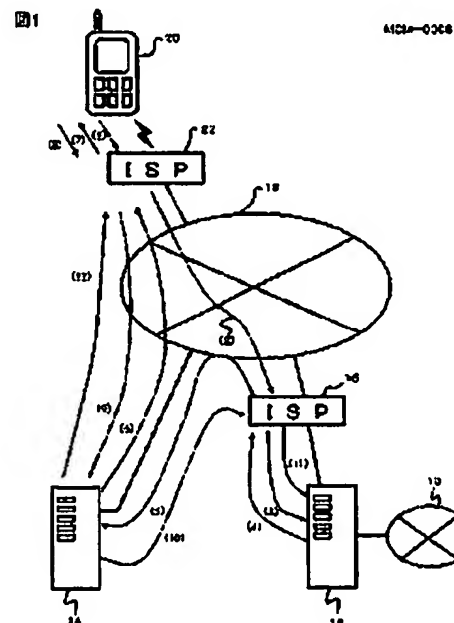
K401 K404 K406 L802 LC13

(54)【発明の名称】 不正アクセス防止方法及びセキュリティ管理装置及びゲートウェイ装置及び端末装置

(57)【要約】

【課題】 プライベートなネットワークに対する外部からの不正アクセスを防止しうる方法及びその方法を実現する装置を提供する。

【解決手段】 端末20から家庭内ネットワーク10に対するパケットが送信されると、ゲートウェイ装置12は、パケットのパケット情報と、自己認証データとを、セキュリティ管理装置24に送信する。セキュリティ管理装置24は、パケットの送信者に対して認証データを要求する。端末20は要求に応じて認証データを送信する。セキュリティ管理装置24は送られてきた認証データに基づき、送信者が正当な権利を有するか否かを検査し、正当な権利を有していれば、ゲートウェイ装置12に対して、フィルタリングの解除命令を出す。一方、不正なアクセスであると判断した場合は、第2のISP22に対して、警告を通知する。このようにして、アクセスの管理を外部に委託することができる。



BEST AVAILABLE COPY

【特許請求の範囲】

【請求項1】 外部ネットワークと内部ネットワークとをゲートウェイ装置で接続し、前記外部ネットワーク側から、前記内部ネットワーク側の装置に対する不正なアクセスを防止する不正アクセス防止方法において、

前記外部ネットワーク側から、前記内部ネットワーク内の装置に対してデータパケットが送信されてきた場合に、前記データパケットのパケット情報と、前記ゲートウェイ装置の自己認証データと、を前記外部ネットワーク上のセキュリティ管理装置に送信するパケット情報送信ステップと、

前記セキュリティ管理装置が、前記バケット情報に基づき、前記データバケットの送信者に送信者側認証データを要求する要求ステップと、

前記要求に応じて、前記送信者が前記送信者側認証データを前記セキュリティ管理装置に送信する送信者側認証データ送信ステップと、

前記送信されてきた送信者側認証データと、前記ゲートウェイ装置の自己認証データと、に基づき、前記送信者が前記内部ネットワークへのアクセスを許可されているかどうかを判断する認証ステップと、

前記認証ステップの結果、前記送信者が前記内部ネットワークへのアクセスを許可されている場合には、前記セキュリティ管理装置は、前記ゲートウェイ装置に対して、前記データバケットの内部ネットワークへの流入を許可するよう命令する命令ステップと、

を含むことを特徴とする不正アクセス防止方法。

【請求項２】 請求項１記載の不正アクセス防止方法において、

前記認証ステップの結果、前記送信者が前記内部ネットワークへのアクセスを許可されていない場合には、前記セキュリティ管理装置は、前記送信者を管理する管理者に対して、警告を通知する警告通知ステップ、を含むことを特徴とする不正アクセス防止方法。

【請求項3】 請求項1記載の不正アクセス防止方法において、

前記要求ステップを実行した後、所定期間内に前記送信者側認証データが送信されてこなかった場合に、前記セキュリティ管理装置は、前記送信者を管理する管理者に対して、警告を通知する第2警告通知ステップ、

を含むことを特徴とする不正アクセス防止方法。

【請求項4】 請求項1、2又は3記載の不正アクセス防止方法において、

前記外部ネットワークはインターネットであり、前記内部ネットワークは家庭内ネットワークであることを特徴とする不正アクセス防止方法。

【請求項5】 請求項1、2又は3記載の不正アクセス防止方法において、

前記バケット情報は、前記データバケットの送信番地のIPアドレス又はTCP情報又はUDPアクセスポート番

号のいずれかであることを特徴とする不正アクセス防止方法。

【請求項6】 請求項2又は3記載の不正アクセス防止方法において、

前記送信者を管理する前記管理者は、前記送信者が利用するインターネットサービスプロバイダであることを特徴とする不正アクセス防止方法。

【請求項7】 ネットワークを介して接続された他の通信装置の管理を行うセキュリティ管理装置であって、前記ネットワークと接続するインターフェース手段と、前記他の通信装置に対してアクセスを許可された者の認証データが記憶された表を記憶する記憶手段と、

前記他の通信装置から、前記他の通信装置にデータパケットを送信した送信者の認証を依頼された場合に、前記送信者にその者の認証データの送付を依頼し、送付されてきた前記認証データが、前記表に記載されているか否かを検査し、記載されている場合には、前記他の通信装置にアクセスを許可する旨の命令を発する制御手段と、を含むことを特徴とするセキュリティ管理装置。

【請求項8】 請求項7記載のセキュリティ管理装置であって、

前記制御手段は、前記送付されてきた認証データが前記表に記載されていない場合には、前記送信者の管理者に警告を通知することを特徴とするセキュリティ管理装置。

【請求項9】 請求項7記載のセキュリティ管理装置であって、

前記制御手段は、前記認証データの送付を依頼した後、所定期間内に前記認証データが送信されてこなかった場合に、前記送信者の管理者に警告を通知することを特徴とするセキュリティ管理装置。

【請求項10】 請求項7、8又は9記載のセキュリティ管理装置において、

前記ネットワークはインターネットであり、前記他の通信装置はゲートウェイ装置であることを特徴とするセキュリティ管理装置。

【請求項11】 請求項8又は9記載のセキュリティ管理装置において、

前記管理者は、前記送信者が接続するインターネットサービスプロバイダであることを特徴とするセキュリティ管理装置。

【請求項12】 外部ネットワークと内部ネットワークとを接続するゲートウェイ装置であって、

前記外部ネットワークと接続する第1インターフェース手段と、

前記内部ネットワークと接続する第2インターフェース手段と、

前記外部ネットワークから前記内部ネットワークに向かうデータパケットのフィルタリングを行うフィルタリ

ク手段と、

(3)

特許 2002-247111

3

前記フィルタリング手段の制御を行う制御手段であって、前記外部ネットワークから前記内部ネットワークに向かうデータパケットが送信されてきた場合に、前記パケットのヘッダ情報と、ゲートウェイ装置の自己認証データとを他の管理装置に送信し、この管理装置からフィルタリングを解除する旨の命令が送信されてきた場合に、前記フィルタリング手段のフィルタリングを解除し、前記データパケットを前記内部ネットワークへ流すことを許可する制御手段と、

を含むことを特徴とするゲートウェイ装置。

【請求項 13】 請求項 12 記載のゲートウェイ装置において、

前記外部ネットワークは、インターネットであり、前記内部ネットワークは家庭内ネットワークであることを特徴とするゲートウェイ装置。

【請求項 14】 請求項 12 記載のゲートウェイ装置において、

前記パケット情報は、前記データパケットの送信者の IP アドレス又は TCP 情報又は UDP アクセスポート番号のいずれかであることを特徴とするゲートウェイ装置。

【請求項 15】 請求項 12 記載のセキュリティ管理装置において、

前記管理装置は、前記外部ネットワークを介して接続しうるセキュリティ管理装置であることを特徴とするゲートウェイ装置。

【請求項 16】 ネットワークに接続可能な端末装置において、

前記ネットワークに接続するインターフェース手段と、前記ネットワークを介して、他の管理装置から本端末装置側の認証データの送信を要求された場合に、前記認証データを前記他の管理装置に対して送信する制御手段と、

を含むことを特徴とする端末装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、所定のネットワークに対する不正アクセスを防止する方法に関する。さらに、この方法を実現する各種通信機器に関する。

【0002】

【従来の技術】 近年、ネットワークが発達し、家庭内においてもいわゆる家庭内ネットワークが広く利用されている。この家庭内ネットワークにおいては、複数の情報家電製品が互いに接続され、情報の共有等が実現されている。また、この家庭内ネットワークは外部のインターネット等に接続されている場合も多い。

【0003】 さて、この家庭内ネットワークの利用者は、外部からその家庭内ネットワークにアクセスできれば便利である。たとえば、インターネット上からこの家庭内ネットワーク内の情報家電製品にアクセスできれば

4

家庭内ネットワークの情報を外部から取り出すことができ、利便性の高い運用が可能である。特に、近年はインターネットにアクセス可能な携帯電話等が広く普及しており、そのような携帯電話からインターネットを介して家庭内ネットワークにアクセスできれば一層利便性に富む運用が可能である。

【0004】

【発明が解決しようとする課題】 しかしながら、外部から家庭内ネットワークへのアクセスを無制限に認めたのでは、悪意の第三者が家庭内ネットワークに侵入し、その家庭内のプライバシーの侵害等の問題を生じさせるおそれがある。

【0005】 そこで、家庭内ネットワークと外部のインターネット等との間にアクセスを監視する何らかの手段を講じることが望ましい。

【0006】 本発明はこのような課題に鑑みなされたものであり、その目的は、プライベートなネットワークに対する外部からの不正アクセスを防止する方法及びその方法を実現する装置を提供することである。

【0007】

【課題を解決するための手段】 上記課題を解決するために、本発明は、外部ネットワークと内部ネットワークとをゲートウェイ装置で接続し、前記外部ネットワーク側から、前記内部ネットワーク側の装置に対する不正なアクセスを防止する不正アクセス防止方法において、前記外部ネットワーク側から、前記内部ネットワーク内の装置に対してデータパケットが送信されてきた場合に、前記データパケットのヘッダ情報と、前記ゲートウェイ装置の自己認証データと、を前記外部ネットワーク上のセキュリティ管理装置に送信するパケット情報送信ステップと、前記セキュリティ管理装置が、前記パケット情報に基づき、前記データパケットの送信者に送信者側認証データを要求する要求ステップと、前記要求に応じ、前記送信者が前記送信者側認証データを前記セキュリティ管理装置に送信する送信者側認証データ送信ステップと、前記送信されてきた送信者側認証データと、前記ゲートウェイ装置の自己認証データと、に基づき、前記送信者が前記内部ネットワークへのアクセスを許可されているか否かを判断する認証ステップと、前記認証ステップの結果、前記送信者が前記内部ネットワークへのアクセスを許可されている場合には、前記セキュリティ管理装置は、前記ゲートウェイ装置に対して、前記データパケットの内部ネットワークへの流入を許可するよう命令する命令ステップと、を含むことを特徴とする不正アクセス防止方法である。

【0008】 このような構成によって、内部ネットワークにアクセスする正当な権利を有する者が内部ネットワークにデータパケットを送信することができる。

【0009】 また、本発明は、前記認証ステップの結果、前記送信者が前記内部ネットワークへのアクセスを

BEST AVAILABLE COPY

れる。

【0031】また、本発明は、前記外部ネットワークは、インターネットであり、前記内部ネットワークは家庭内ネットワークであることを特徴とするゲートウェイ装置である。

【0032】このような構成によって、インターネットから家庭内ネットワークに対してなされるアクセスが正当なものか否かの判断を外部に委託することができる。

【0033】また、本発明は、前記バケット情報は、前記データバケットの送信者のIPアドレス又はTCP情報又はUDPアクセスポート番号のいずれかであることを特徴とするゲートウェイ装置である。

【0034】このような構成によって、送信者を識別する情報としてIPアドレス等を利用することができる。

【0035】また、本発明は、前記管理装置は、前記外部ネットワークを介して接続しうるセキュリティ管理装置であることを特徴とするゲートウェイ装置である。

【0036】このような構成によって、セキュリティ管理装置は、内部ネットワーク内に対するアクセスをすることなく送信音が正当なものであるか否かの判断を行うことができる。

【0037】また、本発明は、ネットワークに接続可能な端末装置において、前記ネットワークに接続するインターフェース手段と、前記ネットワークを介して、他の管理装置から本端末装置側の認証データの送信を要求された場合に、前記認証データを前記他の管理装置に対して送信する制御手段と、を含むことを特徴とする端末装置である。

【0038】このような構成によって、認証データを管理装置に送信することができる。

【0039】

【発明の実施の形態】以下、本発明の好適な実施の形態を図面に基づいて説明する。

【0040】実施の形態1

図1には、本施設の形態1の通信システムの全体構成図が示されている。

【0041】この図に示すように、本実施の形態1においては、家庭内ネットワーク10は、ゲートウェイ装置12を介して第1のインターネットサービスプロバイダ16に接続している。そして、この第1のインターネットサービスプロバイダ16を介して、インターネット18に接続している。なお、図1においては、インターネットサービスプロバイダは「ISP」と簡略した記載となっている。

【0042】この家庭内ネットワーク10に外部からアクセスしようとする者の端末20は、第2のインターネットサービスプロバイダ22に接続している。そして、この第2のインターネットサービスプロバイダ22を介して、上記端末20はインターネット18に接続されている。第2のインターネットサービスプロバイダ22

も、図1においては、簡略した記載「ISP」としている。以下、インターネットサービスプロバイダはしばしば「ISP」と記す。

【0043】家庭内ネットワークに外部から接続しようとする場合としては、その家庭の人が外から、家庭内部の情報を知りたいと思う場合が典型的な例としてあげられよう。

【0044】この場合の端末20は、たとえばパーソナルコンピュータが考えられる。また近年はインターネット18に接続しうる携帯電話等も多く利用されているため、端末20として携帯電話等の各種モバイル通信機器を利用することも考えられる。なお、端末20は、本発明の「端末装置」に相当する。

【0045】また、インターネット18にはセキュリティ管理装置24が接続されている。このセキュリティ管理装置24は、ゲートウェイ装置12毎に、そのゲートウェイ装置12に対するアクセスを管理している。

【0046】このセキュリティ管理装置24には、自分が管理するゲートウェイ装置12の自己認証データと、このゲートウェイ装置12に対してアクセスが許可されている端末20の認証データとを記載した表（データベース）が格納されている。このような表の概念図が図2に示されている。この図に示すように、この表は、ゲートウェイ装置12毎に設けられた表であって、ゲートウェイ装置12に対してアクセスが許可されている端末20の認証データを記載した表である。

【0047】なお、図末20の認証データは、本発明の「送信者側認証データ」や「図末装置側の認証データ」に相当する。

【0048】次に、態様20から家庭内ネットワーク10へのアクセスの動作について説明する。図3には、この際の動作の流れを表すフローチャートが示されている。

【0049】まず、ステップS3-1においては、端末20から家庭内ネットワーク10に対するデータパケット（以下、単にパケットと呼ぶ）が送信される。このパケットは、まず第2のISP22に到着する（図1中（1）で示される）。続いて、パケットは、第2のISP22から、インターネット18を通過して、第1のISP14に到着（図1中（2）で示される）する。そして、パケットは、第1のISP14から家庭内ネットワーク10のゲートウェイ装置12に到着する（図1中（3）で示される）。

【0050】ステップS3-2においては、ゲートウェイ装置12が、送られてきた上記パケットのパケット情報と、自己認証データとを、セキュリティ管理装置24に送信する。このデータは、まず第1のISP16に到着し(図1中(4)で示される)、さらにインターネット18を経由してセキュリティ管理装置24に到着する(図1中(5)で示される)。

【0051】ここで、自己認証データとは、ゲートウェイ装置12が自己を表すためのデータであり、セキュリティ管理装置24は、この自己認証データを用いてどのゲートウェイ装置12であるかを識別することができる。また、パケット情報とは、上記パケットを送信した者(送信者)を特定できるデータであって、IPアドレスや、TCPやUDPのアクセスポート番号、又はパケットの内容等を利用することができる。

【0052】ステップS3-3においては、セキュリティ管理装置24が、上記パケット情報に基づきパケットの送信者を特定し、その送信者に対して認証データを要求する。この要求のメッセージはインターネット18を介して第2のISPに到着し(図1中、(6)で示される)、第2のISPから端末20に送信される(図1中、(7)で示される)。

【0053】ステップS3-4からは、端末20が上記要求に応じて認証データを送信するか否かによって、処理が分岐する。認証データを送信する場合には、ステップS3-5に処理が移行する。一方、何らかの理由により、認証データを送信できない場合は、セキュリティ管理装置24は認証データを受信できない。セキュリティ管理装置24が所定期間内に認証データを受信できなかった場合には、ステップS3-8に処理が移行する。

【0054】ステップS3-5においては、端末20からセキュリティ管理装置24に対して認証データが送信される。この認証データはまず、端末20から第2のISPに送られ（図1中、(8)で示される）、続いて、インターネット18を介してセキュリティ管理装置24に到着する（図1中、(9)で示される）。

【0055】ステップS3-6においては、セキュリティ管理装置24が送られてきた上記認証データに基づき、送信者がゲートウェイ装置12に対してアクセスする権利を有するか検査される。この検査は、図2で説明した表を検索することによって実行される。まず、セキュリティ管理装置24は、ゲートウェイ装置12の自己認証データに基づき、そのゲートウェイ装置12の表を見つけた（図2）。次に、その表中に、パケットの送信者が送信してきた認証データが存在するか否かを検査する。この検査の結果、表中に上記認証データが存在すれば、そのパケットの送信者はそのゲートウェイ装置12を介して家庭内ネットワーク10にアクセスする正当な権利を有していると判断し、ステップS3-7に処理が移行する。一方、上記表中に認証データが存在しない場合には、そのパケット送信者は正当な権利を有していないと判断し、ステップS3-8に処理が移行する。

【0056】ステップS3-7においては、セキュリティ管理装置24は、ゲートウェイ装置12に対して、フィルタリングの解除命令を出す。この解除命令は、インターネット18を介して第1のISP16に到達し(図1の10)で示される)。第1のISP16からゲ

トウェイ装置12に到達する(図1の(11))で示される)。この解除命令を受けて、ゲートウェイ装置12はパケット送信者が送信してきたパケットを東席内ネットワーク10に供給する。

【0057】一方、ステップS3-8においては、セキュリティ管理装置24は、不正なアクセスであると判断し、パケットの送信者が接続している第2のISP22に対して、警告を通知する(図1の(12)で示される)。先に述べたように、このステップS3-8において警告が通知されるのは、認証データを所定期間内にセキュリティ管理装置24が受信できなかった場合、もしくは、認証データが正しくなかった(表中になかった)場合、のいずれかの場合である。

【0058】以上述べたように、本実施の形態1によれば、家庭内ネットワーク10にアクセスする権利を有する者に対してのみ家庭内ネットワーク10への流入を許可することができる。特に、その判断を外部のセキュリティ管理装置24に委託することができるため、ゲートウェイ装置12自身の負担を減らすことができるというメリットがある。

【0059】さらに、不正なアクセスを排除するだけでなく、不正なアクセスがあった場合には、ISPに対して警告を通知するので、不正行為の抑止効果を期待することができる。

【0060】セキュリティ管理装置の構成

次に、セキュリティ管理装置24の構成を図4に基づいて説明する。この図に示すように、セキュリティ管理装置24は、上述した図2で示す表を管理するゲートウェイ装置12の個数だけでなく記憶している記憶手段40を備えている。また、インターネット18と接続するためのインターフェース42を備えている。さらに、図3で説明した動作を実行する制御手段44を備えている。

【0061】制御手段44は、プログラムとそのプログラムを実行するプロセッサとから構成されており、このプログラムによって、上述した各動作の制御が行われる。

【0062】(1)すなわち、外部のゲートウェイ装置12から、その自己認証データと、ゲートウェイ装置12に送信されたパケットのパケット情報と、がインターフェース42を介してセキュリティ管理装置24に送信されてきた場合に、そのパケット情報に基づきパケットの送信者に認証データを要求する。そして、認証データを受信する。

【0063】(2)次に、上記自己認証データからそのゲートウェイ装置12の表を見つけ、その表中に上記認証データが存在するか否かを検査する。

【0064】(3)表中に設定データが存在すれば、ゲートウェイ装置12にパケットに対するフィルタリングを解除し、パケットを家庭内ネットワーク10に流入することを許可するよう命令する。

【0065】(4)一方、表中に認証データが存在しない場合や、所定時間内に認証データが送られてこなかった場合には、パケット送信者の管理者に警告を通知する。

【0066】なお、記憶手段40は、ハードディスク等の各種の磁気ディスク、又はCDROM、DVDROM等の各種の光ディスク等、種々の記憶手段を利用することができる。また、セキュリティ管理装置24は、複数のゲートウェイ装置12を管理することができる。その場合には、記憶手段40内に、複数のゲートウェイ装置12毎に作成された複数の表が格納される。

【0067】ゲートウェイ装置の構成

次に、ゲートウェイ装置12の構成を図5に基づいて説明する。この図に示すように、ゲートウェイ装置12は、家庭内ネットワーク10に接続するためのインターフェース50と、インターネット18に接続するためのインターフェース52とを備えている。

【0068】また、ゲートウェイ装置12は、インターネット18側からやってきたパケットをフィルタリングするフィルタリング手段54を備えている。このフィルタリング手段54は、家庭内ネットワーク10からインターネット18に向かうパケットのフィルタリングも行う。

【0069】ゲートウェイ装置12は、制御手段56を有している。この制御手段56は、フィルタリングの対象となるパケットの定義や、フィルタリングの内容等を設定する手段であり、プログラムとそのプログラムを実行するプロセッサによって構成されている。

【0070】また、このプログラムによって、制御手段56は、上述した図3で説明した動作を実行する。

【0071】(1)すなわち、インターネット18からパケットがインターフェース52を介して送信されてきた場合には、そのパケット情報と、自己認証データとを、外部のセキュリティ管理装置24に送信する。ここで、自己認証データは、ゲートウェイ装置12を識別可能なデータであればどのようなデータでもかまわない。

【0072】(2)次に、上記セキュリティ管理装置24から、フィルタリングの解除命令が送信されてきた場合には、上記フィルタリング手段54を制御して、家庭内ネットワーク10への流入を許可するのである。

【0073】(3)このような解除命令が来ない限り、フィルタリング手段は上記パケットをフィルタリングし続ける。すなわち、家庭内ネットワーク10への流入を許可しないのである。このようにして不正なアクセスによるパケットの流入を防止することが可能である。

【0074】なお、フィルタリング手段54はソフトウェアで構成することも好ましいが、性能を向上(処理速度を向上)させるために、ハードウェアで構成することも好ましい。インターフェース50、52はネットワークとのインターフェース手段として既存の構成をそのま

ま利用可能である。

【0075】端末の構成

次に、端末20の構成を図6に基づいて説明する。この図に示すように、端末20は、第2のISP22と接続するためのインターフェース60を備えている。

【0076】また、端末20は、利用者に所定の情報を表示するための表示手段62や利用者が情報を入力するための入力手段64を備えている。これらの表示手段62や入力手段64は従来からよく知られた構成である。

【0077】さらに、端末20は、制御手段66を備えている。この制御手段66は、プログラムとそのプログラムを実行するプロセッサによって構成されている。そして、このプログラムによって、制御手段66は、上述した図3で説明した動作を実行する。すなわち、制御手段66は、インターネット18を介して、セキュリティ管理装置24から、端末20の認証データを要求された場合に、その要求に応じて認証データをセキュリティ管理装置24に送信するのである。

【0078】実施の形態2

上記実施の形態1では、家庭内ネットワーク10の例を示したが、プライベートなネットワークであればどのようなネットワークでもかまわない。また、実施の形態1では、インターネット18の例を示したが、もちろんどのようなネットワークでもかまわない。どのようなネットワークでも本発明を適用することは容易である。

【0079】また、実施の形態1では、パケットの送信者がISPを通じてアクセスする場合について説明したが、ISPを介さずにネットワークに接続する形態でもかまわない。この場合は、管理者としては、ISPではなく、たとえばその送信者の上司や、送信者の所属する団体等が適切である。セキュリティ管理装置24は、ISPの代わりに、これら上司や、団体に対して警告を通知することになる。

【0080】また、ゲートウェイ装置12も第1のISP16を介さずに直接ネットワークに接続する形態であっても本発明を同様に適用することが可能である。

【0081】

【発明の効果】以上述べたように、本発明によれば、外部ネットワークから内部ネットワークへ正当なアクセスのみを許可することができる。また、正当な者からのアクセスか否かを内部ネットワークと外部ネットワークを接続するゲートウェイ装置以外の管理装置に委託することができるため、ゲートウェイ装置の管理負担が減少する。

【0082】特に、認証データを用いて正当な権利を有するものか否かを判断し、認証データが送信者側から送られてこなかった場合、認証データが不正なものであった場合に、不正アクセスが行われたと判断することができる。

【0083】また、不正なアクセスであると判断した場

13

台には、管理者に警告が通知されるため、不正アクセスを将来的にも防止する効果が期待される。また、管理者がインターネットサービスプロバイダである場合には、インターネットサービスプロバイダはそのユーザに不正アクセスを使用した者がいることを知ることができ、ユーザの管理を強化する効果が得られる。

【0084】さらに、セキュリティ管理装置からの要求に応じて認証データが送信されるように端末装置を構成したので、自己が内部ネットワークに対して正当にアクセスをする権利を有する者であることを容易に証明することができ、外部ネットワークから内部ネットワークへのアクセスを円滑に行うことが可能となる。

【図面の簡単な説明】

【図1】本実験の形態1の通信システムの全体構成図である。

【図2】セキュリティ管理装置に格納されている表の概念図である。

【図3】端末から家庭内ネットワークへのアクセスの動作の流れを表すフローチャートである。

【図4】セキュリティ管理装置の構成ブロック図であ
る。 *

14

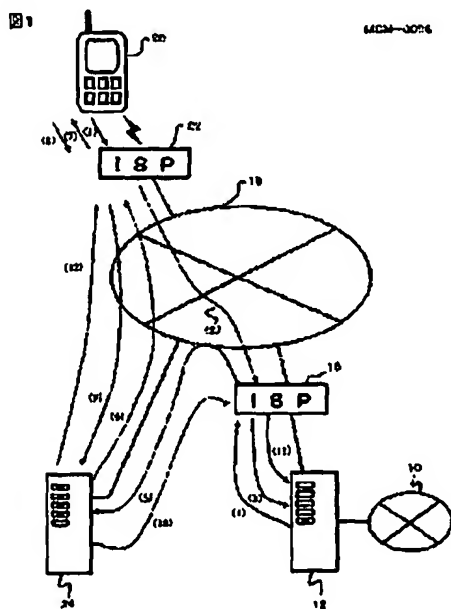
*【図5】ゲートウェイ装置の構成ブロック図である。

【図6】 終末の構成ブロック図である。

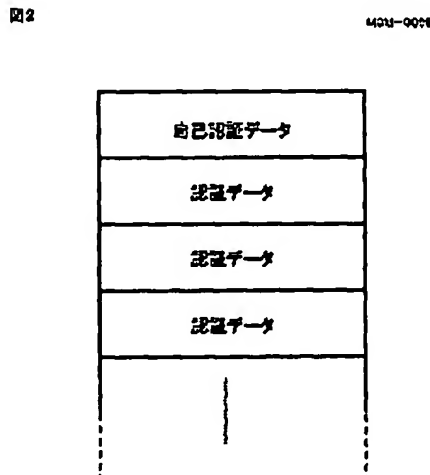
【符号の説明】

- 10 家庭内ネットワーク
- 12 ゲートウェイ装置12
- 18 第1のインターネットサービスプロバイダ
- 18 インターネット
- 20 総末
- 22 第2のインターネットサービスプロバイダ
- 24 セキュリティ管理装置24
- 40 記憶手段
- 42 インターフェース
- 44 制御手段
- 50 インターフェース
- 52 インターフェース
- 54 フィルタリング手段
- 56 制御手段
- 60 インターフェース
- 62 表示手段
- 64 入力手段
- 66 制御手段

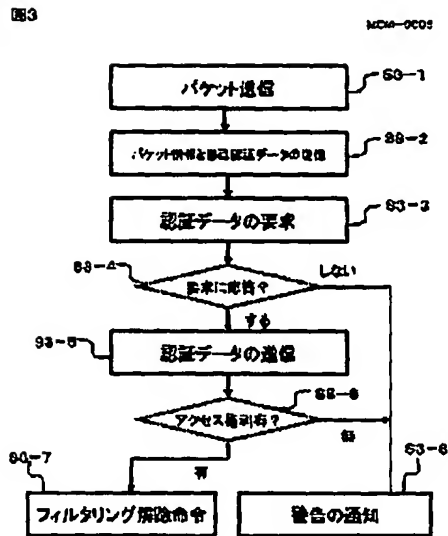
【圖1】



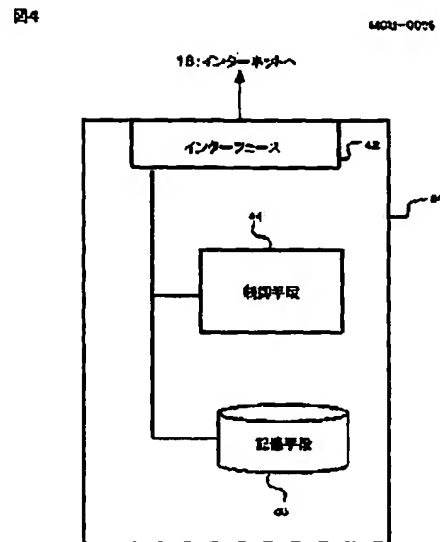
【圖2】



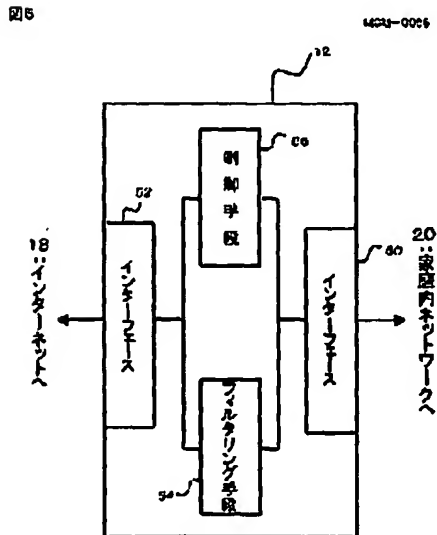
【図3】



【図4】



【図5】



【図6】

